




INFORMATION SECURITY DIVISION

Mississippi's Cyber Security Alert Indicator

Today's Cyber Security Alert is:  **LOW**

What is the Alert Indicator?

The Alert Indicator shows the current level of malicious cyber activity and reflects the potential for, or actual damage. The indicator consists of 5 levels:


1.  **LOW** Indicates a low risk. No unusual activity exists beyond the normal concern for known hacking activities, known viruses or other malicious activity.

Examples:

- Normal probing of the network
- Low risk viruses

Actions:

- Continue routine preventative measures including application of vendor security patches and updates to anti-virus software signature files on a regular basis.
- Continue routine security monitoring.
- Ensure personnel receive proper training on Cyber Security policies.

2.  **GUARDED** Indicates a general risk of increased hacking, virus or other malicious activity. The potential exists for malicious cyber activities, but no known exploits have been identified, or known exploits have been identified but no significant impact has occurred.


Examples:

- A critical vulnerability is discovered but no exploits are reported.

- A critical vulnerability is being exploited but there has been no significant impact.
- A new virus is discovered with the potential to spread quickly.
- Credible warnings of increased probes or scans.
- Compromise of non-critical system(s) that did not result in loss of data.

Actions:

- Continue recommended actions from previous level.
- Identify vulnerable systems.
- Implement appropriate counter-measures to protect vulnerable systems.
- When available, test and implement patches, install anti-virus updates, etc. in next regular cycle.


3.  **ELEVATED** Indicates a significant risk due to increased hacking, virus or other malicious activity which compromises systems or diminishes service. At this level, there are known vulnerabilities that are being exploited with a moderate level damage or disruption, or the potential for significant damage or disruption is high.

Examples:

- An exploit for a critical vulnerability exists that has the potential for significant damage.
- A critical vulnerability is being exploited and there has been moderate impact.
- Compromise of secure or critical system(s) containing sensitive information.
- Compromise of critical system(s) containing non-sensitive information if appropriate.
- A virus is spreading quickly throughout the Internet causing excessive network traffic.
- A distributed denial of service attack.

Actions:

- Continue recommended actions from previous levels.
- Identify vulnerable systems.
- Increase monitoring of critical systems.
- Immediately implement appropriate counter-measures to protect vulnerable critical systems.
- When available, test and implement patches, install anti-virus updates, etc. as soon as possible.


4.  **HIGH** Indicates a high risk of increased hacking, virus or other malicious cyber activity which targets or compromises core infrastructure, causes multiple service outages, multiple system compromises or compromises critical infrastructure. At this level, vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption is high.

Examples:

- An exploit for a critical vulnerability exists that has the potential for severe damage.
- A critical vulnerability is being exploited and there has been significant impact.
- Attackers have gained administrative privileges on compromised systems.
- Multiple damaging or disruptive virus attacks.
- Multiple denial of service attacks against critical infrastructure services.

Actions:

- Continue recommended actions from previous levels.
- Closely monitor security mechanisms including firewalls, web log files, anti-virus gateways, system log files, etc. for unusual activity.
- Consider limiting or shutting down less critical connections to external networks such as the Internet.
- Consider isolating less mission critical internal networks to contain or limit the potential of an incident.
- Consider use of alternative methods of communication such as phone, fax or radio in lieu of e-mail and other forms of electronic communication.
- When available, test and implement patches, anti-virus updates, etc. immediately.

5.  **SEVERE** Indicates a severe risk of hacking, virus or other malicious activity resulting in wide-spread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors. At this level, vulnerabilities are being exploited with a severe level or wide spread level of damage or disruption of Critical Infrastructure Assets.

Examples:

- Complete network failures.
- Mission critical application failures.
- Compromise or loss of administrative controls of critical system.
- Loss of critical supervisory control and data acquisition (SCADA) systems.
- Potential for or actual loss of lives or significant impact on the health or economic security of the State.

Actions:

- Continue recommended actions from previous levels.
- Shutdown connections to the Internet and external business partners until appropriate corrective actions are taken.
- Isolate internal networks to contain or limit the damage or disruption.
- Use alternative methods of communication such as phone, fax or radio as necessary in lieu of e-mail and other forms of electronic communication.